CONCEPTION DE SCENARIOS D'ATTAQUE[1] DE SYSTÈMES[2] COMPLEXES

Exercices de validation de stratégies de protection[3] ou de réaction offensive[4]

G. BOUGET, J-P CHAPUIS, J-G VINCENT

LGST4D 59, Rue des Cailloux 45430 MARDIE

g.bouget@lgst4d.com; j-p.chapuis@lgst4d.com; j-g.vincent@lgst4d.com

Résumé – La génération de scénario pour des exercices ou pour la gestion de crise est une entreprise multi facettes. Elle se doit de permettre l'exploration des objectifs de l'exercice envisagé ou du résultat final recherché dans la résolution d'une crise. Dans nos sociétés modernes, tout est interdépendant et l'évolution d'un seul élément peut aboutir à des changements brutaux voire irréversibles: souvenons-nous des croissants de Marie-Antoinette en période de disette alimentaire qui a amené le 14 juillet 1789 et une évolution irréversible à long terme des mentalités vers les systèmes électifs. Il est désormais impératif de construire des scénarios « intelligents » qui lors de leur génération utiliseront la simulation. Ils intégreront des évènements/incidents favorisant l'étude des interactions entre systèmes en situation dégradée et créant des conditions propices au dialogue avec les vouloirs politiques par la prise en compte dans la gestion de crise des problématiques de reconstruction des services, des infrastructures et des liens sociaux dès le début d'un exercice.

Abstract – Scenario generation for exercises is a multi-facetted task. The scenario must achieve two goals: to explore the objectives of the exercise and the end result of the crisis resolved. In our modern societies so much is interdependent and the evolution of only one element of a crisis can result in brutal, even irreversible, changes. Remember Marie-Antoinette's croissants during France's food shortages which led to the 14th of July 1789, and the irreversible evolution of long term mentalities regarding the governance of the country. Today, it is imperative to construct "intelligent" scenarios using simulation. Scenarios which integrate from the very beginning of the exercise, events and incidents which promote the study of interacting systems in a degrading situation, and which create the necessary conditions for dialogue between the political powers, the reconstruction of essential services, infrastructure and social networks.

---

[1] Attaque : toute intervention interne ou externe, d'origine naturelle, matérielle ou humaine à même d'affecter à court, moyen ou long terme la sécurité et le bien être des citoyens.

[2] Dans le cadre de cet article on appelle « système » une technologie, un ensemble d'objets et toute forme d'organisation sociétale (gouvernement et ses appendices, collectivités locales, associations) concourant à rendre un service précis (transport, communication, collecte, traitement et distribution d'informations, production d'énergie, santé, police, équipe de sports collectifs etc.) . Le terme « système » désigne un objet d'étude artificiel ou naturel, immergé dans un environnement doté de propriétés intrinsèques et changeantes.

3 La stratégie défensive inclue toute les actions visant à renforcer la résilience d'un système humain ou technique ainsi que les infrastructures ; elle englobe également les plans de secours dans l'urgence.

[4] La réaction offensive vise à la réduction, voire à l'élimination d'une menace ou d'une attaque.

1. Liminaire

La validation des plans de protection et de défense (sphère publique ou entreprises) dépend principalement de la qualité des exercices visant à les tester. Les scénarios (cadre spatio-temporel dont les points clefs sont reliés par un script décrivant le déroulement des attaques) se devraient d'être élaborés selon une approche systémique.

L'intégration dans ces scénarios d'évènements et d'incidents favorisant l'étude des interactions entre systèmes dans une situation dégradée établira des conditions propices au dialogue entre vouloirs politiques par la prise en compte des problématiques liées à la reconstruction des services, des infrastructures et des liens sociaux et ce, dès le début d'un exercice.

Qu'en est-il lorsqu'un évènement majeur met à mal les plans et la conduite des opérations par débordement des capacités qu'elles soient privées ou publiques, par rupture des chaines de commandement et du lien social ?

L'exposé ci-après présente succinctement les principaux modes de fonctionnement des organisations de sécurité ; il introduit les systèmes complexes, rouages et composants essentiels de nos sociétés modernes ; après une courte note sur les exercices, il initie des éléments de réflexion pour la construction de scénarios dédiés à l'organisation d'exercices impliquant de multiples systèmes ou à une réaction offensive/préventive face à des attaques concertées.

2. Sécurité, Organisation.

A fin de faire face à la diversité des attaques possibles, d'origine naturelle, technologique ou humaines, à leur fréquence, leur ampleur et leur distribution géographique, de nombreuses organisations internationales (intergouvernementales ou non gouvernementales) ainsi que les états ont mis en place des stratégies en vue de limiter les dommages causés tant aux populations qu'à l'environnement.

Certaines des organisations sont dotées de mandats spécifiques leur donnant des compétences globales, dans des domaines bien définis, par exemple l'Organisation Mondiale de la santé, l'Agence Internationale de l'Energie atomique, l'Organisation Maritime Internationale, l'Organisation Internationale de l'Aviation civile.

Au regard de la spécificité des actions et des programmes mis en œuvre par l'ensemble des intervenants, les phases et les domaines d'interventions ci-après sont pris en compte :

- la prévention des risques ;
- l'organisation des opérations de secours pour répondre à l'urgence ;
- la réhabilitation en vue de restaurer des conditions de vie acceptables d'une communauté.

Préparation et réalité sont souvent bien différentes. L'entrainement à soutenir une action cohérente, avec un stress et une fatigue grandissante pour tous les acteurs impliqués dans une crise, pendant ces trois phases ne peut être obtenue que par des exercices dont les scénarios intégreront les cadres d'action.

Chaque état ou organisation évolue dans un cadre juridique aux contours divers:

- de lege :
  - gestion interministérielle prévue par la législation. – France-Suisse-Australie.
  - gestion ministérielle par un ministère ou organisme unique spécialisé dans la gestion des risques – USA – Russie – Chine
- de fait :
  - gestion sans mention explicitement contraignante dans la législation – Belgique
  - la coexistence d'une agence d'état spécialisée et de Comités Permanents Nationaux et Internationaux aux attributions se recouvrant.

2.1 France, un modèle hiérarchique.

Les lois n° 2003-239 du 18 mars 2003 pour la sécurité intérieure et n° 2004-811 du 13/08/04 de modernisation de la sécurité civile fixent les cadres juridiques, les principes organisationnels ainsi que les directives politiques concourant à la sécurité finale du citoyen.

Le « corpus » des lois et des textes d'organisation procèdent d'une vision hiérarchique basée sur la multiplication et l'empilement de centres de coordination et de commandement, on y ajoutera la création de Centres de Gestion de Crise au sein de chaque ministère. Cette vision jacobine *élude le recours potentiel aux réseaux sociaux existants* et ne prévoit pas d'organiser la formation en masse du public, mais seulement son information, contrôlée.

Pour autant que l'intégrité des organisations centralisées ne soit pas affectée, que les relations entre elles aient été préalablement testées et organisées, *le modèle est très probablement le plus efficace pour la perception d'une vision globale de la crise en cours* et pour la gestion des ressources dédiées en priorité à la sauvegarde des vies humaines et à la protection puis à la restauration des infrastructures.

2.2 Belgique, un modèle d'accords non juridiquement contraignants.

Outre le pouvoir fédéral, la Belgique connaît trois Communautés (française, flamande et germanophone) et trois Régions (Wallonie, Flandre et Bruxelles) avec des compétences territoriales. Pour ces raisons, l'organisation belge est complexe, car il n'y a aucune hiérarchie entre ces différents ensembles (l'Etat fédéral, les Régions et les Communautés).

Les textes de base sont l'Arrêté royal du 23 juin 1971 organisant les missions de la sécurité civile et l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise. Ces deux arrêtés font actuellement l'objet d'études de fond pour leur adaptation à l'évolution des accords et directives internationales.

En matière de gestion des risques, l'Etat fédéral et les trois Régions sont concernés. Trois grands blocs de compétences peuvent être distingués :

- protection de l'environnement : compétence régionale par les Ministères régionaux de l'Environnement ;
- protection de la population : compétence fédérale exercée par le Service Public Fédéral Intérieur, pour la planification d'urgence et la gestion de crise ;
- protection des travailleurs : compétence fédérale parle Service Public Fédéral Emploi et Travail.

Lorsque les compétences sont partagées, les différents niveaux sont parfois obligés de conclure des accords de coopération ;

- l'Accord de coopération du 21 juin 1999 entre l'Etat fédéral, les Régions flamande et wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant les substances dangereuses.
- le plan PLUIES de la Région Wallonne qui réunit 5 domaines d'activités pour lutter contre les inondations et leurs effets.

Sans rentrer dans leurs détails, ces deux accords montrent qu'il est possible de réunir plusieurs autorités concernées sans aucune hiérarchie entre elles pour réaliser des objectifs communs ;

On notera toutefois, qu'en cas d'attaque majeure à même de déborder le cadre de ces deux accords le Centre gouvernemental de Coordination et de Crise serait activé.

2.3 La coopération européenne en matière de protection civile.

Au niveau européen, la protection civile repose sur un mécanisme communautaire dont les fondements ont été mis en place par la Commission en octobre 2001. Ce mécanisme comprend un ensemble de règlements, d'instruments, de normes (transports maritimes, aériens et terrestres, infrastructures) et de systèmes d'action rapide (RAS en anglais) afin d'améliorer la préparation des pays impliqués et de faciliter l'assistance mutuelle en cas de catastrophe.

Ces systèmes se basent sur un réseau d'échange d'informations permettant de recevoir et de déclencher l'alerte ainsi que de faire circuler l'information. Parmi ces systèmes, on peut citer:

- le MIC, Centre de suivi et d'information destiné à organiser et à soutenir l'assistance mutuelle entre les pays participants ;
- le système ECURIE, en cas d'urgence radiologique ;
- BICHAT, pour les attaques et les menaces biologiques et chimiques ;
- RAPEX et le RASFF, pour la santé des consommateurs ;
- EWRS, pour les maladies contagieuses ;
- EUROPHYT, réseau phytosanitaire pour intercepter les organismes nuisibles pour les végétaux ;
- SHIFT, contrôles sanitaires sur les importations ayant des implications vétérinaires ;
- ADNS, pour la santé animale ;
- un réseau d'alerte pour les infrastructures critiques, appelé CIWIN ;
- système d'information Europol ;
- système d'information rapide sur les infrastructures critiques ;
- centre de situation conjoint de l'UE (2005) et le réseau interne d'alerte ARGUS qui dispose d'un centre de crise central regroupant les représentants des services de la Commission concernés par une situation d'urgence.

2.4 Les entreprises.

Certaines entreprises et établissements publics sont tenus d'organiser des exercices : ports, aéroports, tunnels et celles soumises à la directive SEVESO II.

Les opérateurs d'importance vitale (voir Code de la défense et décrets pris en application de l'article L.1332-1 et suivants) doivent concevoir un système de sécurité à deux étages : un plan de sécurité pour l'ensemble de leurs activités relevant du ou des secteurs traités, et des plans particuliers de protection pour chacun de ses points d'importance vitale.

Un projet de directive européenne sur la protection des infrastructures vitales européennes est en cours de discussion. Son objectif est de fixer certaines obligations de sécurité aux opérateurs d'infrastructures vitales qualifiées d'européennes, c'est-à-dire dont la destruction ou l'avarie aurait un impact transfrontalier significatif.

Nous rajouterons que tous les pays du monde ont (Etats-Unis d'Amérique, Suisse et Russie) ou vont faire établir des plans de sécurité pour leurs installations vitales.

Chaque installation ou réseau est en fait composé d'éléments qui dialoguent entre eux, jusqu'à former un ensemble difficile à appréhender dans sa globalité.

3. Systèmes complexes

3.1 Définitions.

Le terme « système », définit précédemment, désigne en outre, un objet d'étude artificiel ou naturel, immergé dans un environnement doté de propriétés intrinsèques et changeantes.

« On appelle systèmes complexes ceux dont les interactions des composants sont non linéaires (les effets ne sont pas proportionnels à la cause). Il est souvent extrêmement difficile, voire impossible, de prédire directement le comportement global ; tous les constituants concourent simultanément à la dynamique d'un comportement devenu holistique : on doit étudier le système comme un tout et non pas comme un ensemble de parties indépendantes. » (Citation : Jean Lemoigne / Hervé Zwirn).

Habituellement, les systèmes[i] sont pratiquement invisibles à l'usager. Généralement, celui-ci ne perçoit que le service rendu et non le système qui le rend. Il peut s'agir de téléphoner, de regarder la télévision, d'avoir accès à l'eau, au gaz, à l'électricité, de pouvoir mener des transactions, de réserver des voyages etc.

3.2 Dynamique des systèmes.

Qu'il survienne un évènement majeur : grève nationale[ii] ou locale[iii], aléa climatique majeur[iv], défaillance involontaire[v] en un point clé, voire une attaque délibérée et organisée[vi], terroriste ou non… *et l'existence d'un système complexe*[vii] *se révèle derrière la paralysie totale ou partielle d'une fonction* parfois essentielle à la collectivité locale ou nationale[viii], à la survie d'une entreprise[ix] ou d'un groupe social.

Le système défaillant modifie son environnement en induisant des effets positifs et/ou négatifs sur d'autres systèmes ; même si l'impact sur les autres systèmes est à délai court, *les résultats de ces effets sont généralement observés avec un temps de retard* ; ce délai est à même de générer des réactions excessives ou inappropriées

Enfin, dans le cas d'un évènement majeur, on pourra assister à la *réorganisation des structures et l'évolution de systèmes*[x] afin de pourvoir à leur finalité qui est celle de fournir un service. Les réorganisations se feront essentiellement sous trois types de contraintes :

- financières (sauf réquisition) pour les sociétés commerciales ;
- les arbitrages politiques pour les structures de type collectivités publiques et étatiques ;
- les facteurs sociétaux pour les groupes sociaux.

.

La claire perception de ces contraintes est essentielle dans la construction d'un scénario, car elles modèlent les organisations quand elles seront dépassés par les évènement.

On perçoit ici une *dynamique de systèmes complexes*[xi] qui évolue de la résistance à l'agression à la perte de fonctions et au fonctionnement en mode dégradé, puis à la restauration avec éventuellement reconfiguration et/ou création de nouveaux systèmes.

Pour les informaticiens et architectes de systèmes logiciels, on pourrait comparer cette dynamique à celle de deux logiciels synchronisés en mode normal (A demande un service à B, le logiciel B exécute, en retour A reçoit le service demandé, le traite et réémet vers B), et qui du fait d'une agression passerait en mode de fonctionnement asynchrone (A demande un service et attends une réponse, après un délai, même sans réponse A redemande un service).

Le cas le plus dangereux dans le fonctionnement des systèmes complexes en situation dégradée est lié à l'activation de systèmes dormants ou enfouis, car elle s'apparente pour l'utilisateur à la gestion d'une situation dynamique dont il ne connaît ni les composants, ni l'issue.

3.2.1 Les systèmes dormants.

Les systèmes dits dormants restent inactifs ou très peu actifs durant de très longues périodes et sont sollicités ou réveillés de manière aléatoire pour des actions ou des combinaisons d'actions exceptionnelles voire dangereuses.

Disposant de peu d'information sur leur fonctionnement, l'utilisateur éprouve généralement des difficultés à comprendre le comportement du système et à redéfinir son propre comportement face aux modifications du système.

Ce seront principalement les systèmes de sécurité des ensembles industriels (centrales électriques et ouvrages d'art) et des aéronefs. L'entrainement est dès lors impératif pour les opérateurs principalement à partir de simulateurs.

3.2.2 Les systèmes enfouis.

Il s'agit ici de toutes les applications utilisées par un opérateur qui se lancent sans intervention ni contrôle de la part de l'opérateur et donc sans accès à la chaîne causale des informations qui régissent le système. Le danger est

l'incapacité de l'usager à comprendre le comportement du système dans les situations de crises.

3.2.3 Les SCADA.

SCADA est un acronyme de contrôle de surveillance et d'acquisition de données. SCADA se réfère à un système qui recueille des données provenant de divers capteurs, situés parfois à des milliers de km et envoie ces données à un ordinateur central qui gère, contrôle les données, les analyse puis donne des ordres à des composants de travail (niveau d'eau haut : ouvre une vanne ; surcharge électrique locale : commute un réseau ; panne sur une voie ferrée : reconfigure les aiguillages ; etc.).

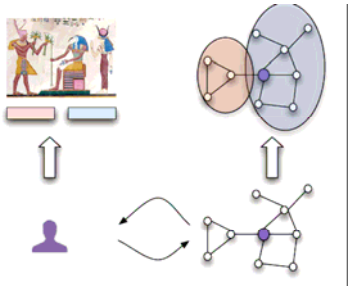
Ce sont principalement des systèmes d'acquisition de données et de contrôle des systèmes de distribution. Ils interviennent dans tous les secteurs de notre vie quotidienne.

3.2.4 Les systèmes coopérants.

Ce sont ceux dont les données peuvent être échangées de manière automatique. Il existe deux modes de fonctionnement : celui dont les données sont libres d'accès et traitées par le système recevant et celui dont les données sont formatées avant mise à disposition d'un autre système préalablement agréé.

Un exemple malheureux récent illustre le résultat de systèmes non-coopérants : services de secours et celui de la Santé. Le premier ne connait pas en temps réels les lits disponibles et leurs emplacements, le second ne connait pas le nombre et le positionnement des ambulances qui réclament ou vont réclamer des lits ; personne ne coordonne, ni n'arbitre entre les priorités.

3.2.5 Les systèmes d'interaction sociétale.



CREA – Ecole Polytechnique

Dans nos études de scénario, nous avons adopté une classification de système (interaction, organisation et société) proche de celle proposée par Luhmann, Niklas (1984), dans son ouvrage Soziale Systeme: Grundriss einer allgemeinen Theorie.

- Le système d'interaction ne permet qu'à un des groupes sociaux de prendre la parole à la fois. Ainsi, le changement de thème ne peut se faire que dans une relation chronologique, au prix d'un temps supplémentaire. Cette linéarité séquentielle condamne ce type de système à ne pouvoir traiter les communications d'ordre plus complexe.
- Le système organisé (organisation sociétale) se constitue autour de règles d'appartenance au système dans des conditions fixées par ses règles. Il exclut ceux qui ne lui appartiennent pas ; le dialogue n'est possible que par un système d'interaction.
- La société est un système d'ordre supérieur qui permet les communications entre absents aussi bien que les communications en face-à-face. « Ses propres frontières sont bordées par les modes de communication possible, elles sont avant tout les frontières de l'accessibilité aux autres et de leur compréhension. » (traduction libre) .

Les systèmes d'interaction sociétale sont complexes et touchent au cœur même des sociétés modernes et en particulier des mégalopoles. Comprendre les interactions, les organisations et les sociétés qui les peuplent devrait permettre la simulation du système sociétal et la création de scénarios de crise intégrant les deux questions ci-après :

- Comment maintenir, voire imposer, les mesures nécessaires au bon fonctionnement des services critiques dans le cas d'une crise ?
- Existe-t-il des seuils à partir desquels la population ne tolèrera plus les failles dans ces services critiques ? Si oui, quels sont ceux qui mettront en péril la stabilité de notre société et le pouvoir de l'Etat ?

4. Simulation.

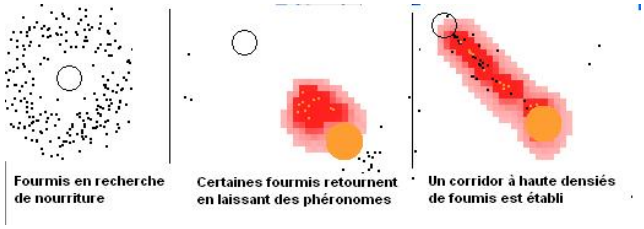
L'évolution de tout objet peut être soit déterministe soit stochastique. Le premier cas peut être traduit dans un logiciel dont la fixation des conditions initiales conduit à une évolution calculable (épandage de produits chimiques ou radiologique). Le second est celui dont le résultat ne peut-être prédit soit parce qu'une petite variation des conditions initiales engendre un résultat à forte variabilité, soit parce que les variables ne peuvent être résolues par un algorithme prédictif (théories du chaos, automate cellulaires et agents intelligents non bornés).

Des exemples illustratifs peuvent être explorés par le lecteur curieux :

- études sur la dynamique des populations[xii],
- le jeu de la vie et ses dérivés, automate cellulaire imaginé par John Horton Conway en 1970, qui est probablement, à l'heure actuelle, le plus connu de tous les automates cellulaires ;
- le modèle des fourmis ; les mouvements de foule pour les agents intelligents.

Toutefois, on notera que des représentations graphiques permettent souvent de détecter des états stables ou des figures répétitives, permettant d'en extrapoler des conclusions valables pour une période déterminée.

Ci-dessous une illustration du modèle des fourmis ; quel que soit la position de la nourriture, on arrivera toujours à établir le corridor. Une extrapolation peut-être faite pour le ravitaillement d'une population où chaque « chercheur » serait muni de l'équivalent technique des phéromones.


Fourmis en recherche de nourriture
Certaines fourmis retournent en laissant des phéronomes
Un corridor à haute densiés de foumis est établi

Avec l'aimable autorisation de Eurobios

5. Les Exercices.

Les retours d'expérience de crise et l'étude de différents exercices et de crises réelles montre à l'envi les limites des plans actuels et futurs en ce qui concerne la phase de fonctionnement des systèmes en mode dégradé. Ce point est le plus critique. A ce jour, seuls les Etats Unis d'Amérique, la Suisse et l'Australie semblent avoir intégré dans leur législation et directives *les dimensions système et facteurs humains locaux* dans la gestion de crise. L'Europe en est encore à étudier la protection des infrastructures critiques[xiii] en les élargissant à la notion de réseaux fonctionnels plus large. La Commission a planifié finance les plans de grande envergure afin d'améliorer la résilience des grandes infrastructures et systèmes vitaux.

Les plans de prévention, de protection, d'intervention et de sécurité établissent et encadrent les différentes actions à mener. *Il y a obligation* pour l'autorité ayant approuvé un plan d'effectuer des exercices pour les valider et pour s'assurer régulièrement de leur pertinence dans un environnement appelé à évoluer. Nous pensons particulièrement aux maires et directeurs d'entreprise qui sont en première ligne tout à la fois au plan règlementaire qu'éventuellement judiciaire pour leur responsabilité pénale en cas d'impréparation Ils sont également moralement responsables vis-à-vis de leurs citoyens ou de leurs employés.

Les exercices – sur table, fonctionnel ou en grandeur nature - devraient permettre aux personnels de s'entrainer à appliquer leurs fiches réflexes, aux responsables de perfectionner la coordination interservices en situation de gestion de crise, *d'appréhender* les problèmes auxquels sont confrontés la population et *sa manière d'y faire face*, de tenter de les aider, puis de faire évoluer les points critiques en fonction de l'analyse du retour d'expérience

Un des meilleurs canevas d'exercice (qui peut très largement être adapté à tout type de situation) est celui de l'IAEA[xiv] ; les méthodes sont également bien décrites par la FEMA[xv] qui intègre les forces sociales locales ; toutefois, seuls les documents de l'OMS[xvi] font référence à la *coordination entre structures organisées et acteurs non spécifiquement formés.*

L'analyse que nous avons menée nous a permis d'identifier plusieurs points faibles dans les exercices que nous avons pu observer (hors exercices militaires).

- Manque de simulation du comportement des individus ou des groupes sociaux et de leur impact sur le fonctionnement des secours ;
- Elaboration des scénarios d'exercices par les cadres de direction qui seront responsables de les conduire puis, ultérieurement, de les analyser ;
- Pas d'analyse réelle interne/externe des scenarii d'exercice ;
- Oubli (volontaire ?) de l'introduction d'un contrôle politique par les élus (maires, collectivités locales et régionales) sur les décisions prises lors d'une gestion de crise dans leurs domaines de responsabilité.

La méthode et les outils utilisés pour la préparation, la conduite et l'exploitation du retour d'expérience devraient constituer un ensemble *normalisé, voire certifié* au sens d'une démarche qualité et évaluation des risques, pour permettre de :

- Créer, organiser, suivre et contrôler un exercice ou une crise militaire, civil ou mixte;
- Vérifier l'état d'avancement des objectifs de l'exercice ou de la maîtrise d'une crise passée;
- Collationner et présenter l'ensemble des données pour l'élaboration des leçons apprises.
- Capitaliser l'ensemble des données issues des précédents exercices ou crises afin de pouvoir les réutiliser.

6. Construction de Scénario.

Toute attaque n'a d'impact réel sur nos sociétés modernes que par ses conséquences politiques, l'ampleur des pertes humaines et les dégâts sur les infrastructures critiques[xvii] qu'elle entraîne.

Les accidents (climatologie et erreurs humaines) peuvent être prévus et la résistance à ce type d'évènements planifiée entrainant une résilience élevée ;

Les attaques d'origine humaines auront pour objectif d'exacerber les tensions entre acteurs humains, après avoir bien étudié les systèmes sociaux ; elles utiliserons toutes les techniques de manipulation de population à même de paralyser le fonctionnement des services de sécurité et

d'aide à la population. La rumeur pointera les dysfonctionnement pour dénigrer les responsables des systèmes de secours et ceux qui détiennent le pouvoir. Elles ajouteront des dégâts ciblés sur les nœuds de communications et les fonctions communes.

Par contre, sous la pression, la puissance publique s'attachera à rendre les systèmes *coopérants*[xviii] lorsque les exercices ou les cas réels auront montré des disfonctionnements ;

Le citoyen et les entreprises tenteront, lorsqu'un système ne fonctionnera plus de trouver un substitut d'abord à moindre coût et ensuite à tous prix et moyens quand leur survie sera en jeu.

Tout scénario se devra d'intégrer les remarques précédentes ainsi que les leçons apprises lors de scénarios antérieurs pour en faire un ensemble cohérent et crédible.

6.1 Définitions.

Un **scénario** est la description d'une séquence de faits dans un cadre spatio-temporel spécifique. L'ensemble forme un tout cohérent lorsqu'un script (synopsis) relie chacun des éléments, l'environnement ayant été décrit. Le scénario conduit à un état final recherché.

Les **évènements** constituent les points clefs d'un scénario ; ils permettent l'initiation de l'évaluation des plans de protection et d'intervention. La **MEL** (Main Events List) est la liste des événements associés à un scénario

Les **incidents** décrivent en détail l'attaque ; ils sont regroupés par événement et par système attaqué. La **MIL** (Main Incidents List) est la liste d'incidents en support des événements. Chacun d'eux appelle une ou plusieurs réactions des joueurs.

Les **réactions** sont les réponses attendues ou les initiatives prises par les joueurs suite à l'injection d'un incident. Lorsque tous les incidents ont été injectés, il est essentiel de vérifier l'ensemble des réactions ; chaque réaction devrait correspondre à un des objectifs d'entrainement.

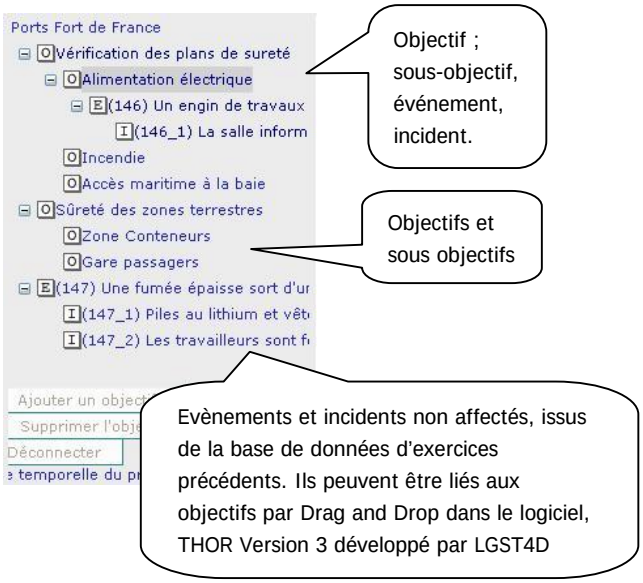
Les **phases** sont des intervalles de temps prédéterminés par le directeur d'exercice ; elles correspondent à des regroupements d'évènements. Deux phases existent toujours :

- La phase d'échauffement qui a pour but d'immerger les joueurs dans l'environnement de l'exercice ; elle permet éventuellement d'activer les plans de précaution.
- La phase de consolidation et de restauration qui permet d'évaluer la pertinence de la mise en œuvre des ressources dédiées à la restauration des services et à la réparation des dommages matériels et psycho-sociaux.

Une troisième phase, celle du retour d'expérience et de consolidation des acquis d'exercices est située hors exercice, mais est indispensable.

Les **ressources** sont constituées par les composants de systèmes physiques, les organisations et les réseaux humains aptes à remplir une fonction ou un service.

Les **objectifs** d'exercices sont l'ensemble des ressources à entrainer, tester et évaluer. Ils sont regroupés par subordination hiérarchique.


Ports Fort de France
Vérification des plans de sureté
Alimentation électrique
(146) Un engin de travaux
(146_1) La salle inform
Incendie
Accès maritime à la baie
Sûreté des zones terrestres
Zone Conteneurs
Gare passagers
(147) Une fumée épaisse sort d'ur
(147_1) Piles au lithium et vêt
(147_2) Les travailleurs sont f
Ajouter un objec
Supprimer l'obj
Déconnecter
e temporelle du pr
Objectif ; sous-objectif, événement, incident.
Objectifs et sous objectifs
Evènements et incidents non affectés, issus de la base de données d'exercices précédents. Ils peuvent être liés aux objectifs par Drag and Drop dans le logiciel, THOR Version 3 développé par LGST4D

6.2 Scénarios.

6.2.1 Conception.

La conception des scenario devrait suivre une approche systémique[xix] basée sur les interactions et relations entre systèmes impliqués par une attaque.

Compte-tenu de l'ensemble des paramètres à intégrer, la création de scénarios doit s'appuyer sur une expertise multidisciplinaire et sur un fonds documentaire le plus complet possible ; l'ensemble se conçoit dans un environnement de travail collaboratif (au sens des portails d'information). C'est ainsi que la quasi-totalité des créateurs de scénarios utilisent des logiciels propriétaires ou commerciaux ainsi que d'outils « open source ».

Un des éléments le plus important est l'adoption d'un Système de Base de Données Relationnelle (SGDBR) flexible, possédant les connecteurs de communications avec d'autres SGDBR et/ou ressources disponibles sur Internet.

L'adoption de XML présente de nombreux avantages en regard des quelques limitations. Tout d'abord, c'est un format texte compris par l'ensemble des logiciels. Il peut être manipulé aisément pour convenir aux imports/exports de données. Ensuite, sa syntaxe et son contenu peuvent être analysés en temps réel, réduisant ainsi sa vulnérabilité aux attaques des outils malveillants.

6.2.2 Etapes de la construction d'un scénario.

Description exhaustive de l'ensemble des objectifs.

Il s'agit avec le concours de la cellule en charge de l'exercice de décrire précisément les moyens et les organisations parties à l'exercice, qu'elles aient un rôle actif ou non.

Création d'une liste d'événements possibles.

Cette liste d'environ 6-7 items, sans chronologie, peut être proposée à partir d'une base de données « évènements » stockée lors de précédents exercices ou créée en fonction du besoin. On notera que si certains évènement sont importés à partir d'une base « historique », une liste d'incidents associés devrait être automatiquement proposée.

Dans tous les cas de figure, les évènements proposés devront impliquer les pouvoirs administratifs, les fonctions régaliennes et l'ordre judiciaires (dommages aux personnes et biens) ainsi que les collectivités locales nationales et/ou transfrontalières. Il s'agit ici d'insérer des sources potentielles de confrontations entre systèmes de natures et de valeurs différentes.

Collecte des données relatives aux joueurs et à l'environnement de l'exercice.

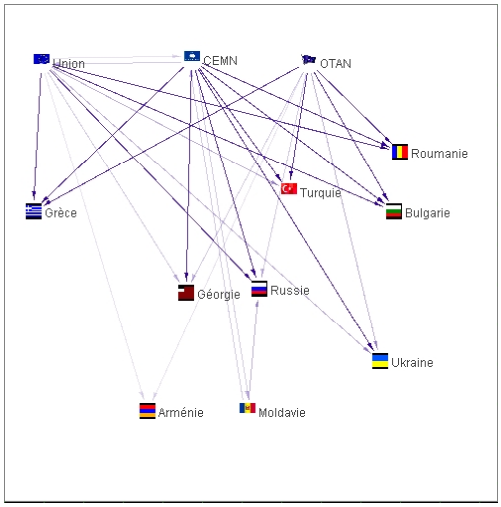
A partir de la liste d'évènements une partie du cadre de l'exercice sera figée ; il convient d'en définir l'environnement ; cet ensemble de données devra être très complet ; il comprendra nécessairement :

- une cartographie – organisée en couches vectorielles dont les données devraient être traduites dans un format Open Geographic Consortium et dont les sources seront issues des principales bases de données nationales et internationales.
- une bibliographie des règlements, accords et traités relatifs à l'exercice ou à la crise ;
- un « qui est qui » regroupé par organisation et réseau social (ces deux points avec représentation graphique) pour pouvoir les organiser en annuaire LDAP.

Il est nécessaire de constituer un ensemble de données parfaitement cohérentes et très exhaustives. Un des principaux problèmes que rencontrent les décideurs lors d'une crise est celui lié à l'afflux de données pertinentes ou non. Il faut donc les entrainer ainsi que leurs collaborateurs à identifier et trier les éléments pertinents à partie de sources diverses structurées ou non; c'est ainsi que l'utilisation d'outils d'analyse de documents, de fouille et de visualisation de données[xx] deviendra familière dans les centres de gestion de crises.

Il s'agit d'inciter les décideurs ou ceux qui leur préparent l'information à utiliser des outils graphiques simples visualisant un état ou son évolution. Le graphique ci-dessous, construit avec le logiciel libre AGNA montre, que l'appel à L'OTAN est une des meilleures options.

Organisation d'un pont aérien massif vers la Bulgarie, l'Ukraine et la Roumanie suite à un désastre majeur - Scénario : météorite dans l'ouest de la Mer noire.



Etude exploratoire LGST4D. Relations politiques en situation d'urgence : la distance entre les drapeaux reflète la force des liens (loi du Chi-2 sur dix paramètres) entre les nations et organisations; l'épaisseur des traits l'intégration des nationaux dans ces organisations.

Description de l'ensemble des systèmes.

Les systèmes doivent être découpés en sous-systèmes, fonctions et liens avec d'autres systèmes. Une approche pourra être d'utiliser les outils et méthodes d'Unified Modelling Langage UML 2.0.

Une attention particulière sera portée à la description des collectivités locales, des associations et des organisations internationales susceptibles d'être impliquées.

Séquence des événements.

Il s'agit d'ordonner les évènements en fonction des interactions entre systèmes et des objectifs d'exercices : montée en puissance des moyens ou au contraire réaction à froid face à un désastre limité ou de grande ampleur.

Simulations initiales.

Elles ont pour but de vérifier l'adéquation entre les bases de données et une séquence d'évènements ; si

nécessaire pour l'exercice ou la réaction à une attaque, on construit un arbre de décision qui prendra en compte plusieurs réactions visibles des systèmes.

Liaison des événements par un script (*synopsis*).

Le script décrit l'enchainement des différents évènements ; il ajoute des détails pertinents ou non à la façon d'un scénario de film qui se déroule, avec éventuellement des retours en arrière. Le script est particulièrement important pendant une phase de phase de stimulation qui peut s'étaler sur plusieurs mois.

Découpage du scénario en phases.

Le script, les évènements, l'environnement et les phases constituent le scénario.

Les phases sont le regroupement dans un même espace de temps de différents évènements, sans lien avec les objectifs de l'exercice, mais avec les conditions propres de son déroulement : temps de travail, montée en puissance des moyens, tempo propre des organisations concernées..

Création des ensembles incidents / réactions attendues.

Chacun des objectifs d'entrainement de l'exercice ou de la réaction offensive correspond à une action attendue suite à l'injection d'incidents. D'une manière générale, on cherchera à saturer par sauts quantitatifs les moyens de réaction et les communications entre eux.

L'organisation des scénarios autour de bases de données trouve ici son utilité. Tous les incidents et actions des exercices ou crises précédentes ayant été capitalisés peuvent être rajoutés et modifiés rapidement pour s'ajuster aux réactions attendues, à chaud.

Vérification cohérence/réactions avec les objectifs.

Le scénario doit comprendre une grille d'évaluation des réactions et pouvoir inclure des actions non prévues (d'initiative des joueurs) dans sa structure. Celles-ci serviront à injecter de nouveaux incidents puisque des initiatives inattendues peuvent être à l'origine de dysfonctionnements.

Relier les incidents aux événements.

Les incidents existent en tant qu'objets indépendants ; par exemple, le type d'incident « incendie de local technique à produits dangereux » peut être appliqué à plusieurs évènements ou systèmes. On peut vouloir évaluer le fonctionnement des services d'incendie dans le cas de feux multiples, mais le type d'incident reste le même.

Dans un scénario de pandémie, il peut y avoir plusieurs évènements ou épisodes infectieux dans des pays différents ; l'incident (découverte de malades dans une école) et les actions à mener sont les mêmes.

Vérification de l'ensemble des chronologies.

Il s'agit d'un test de cohérence obligatoire

Mise en place des éléments post crise ou de reconstruction

Déterminer la période à laquelle débute la phase de réhabilitation n'est pas toujours aisé : quand les actions cessent d'être un simple palliatif pour s'intéresser au plus long terme ? L'expérience montre qu'il n'y a pas de réelle rupture entre la période de réhabilitation et les phases précédentes; il en est de même pour la période de remise en état dont l'un des objectifs est de se préparer à de nouvelles catastrophes : la prévention et la préparation en constituent un aspect important.

Ces éléments doivent être disséminés tout au long du scénario par des incidents qui couvriront toute spectre sociétal : plaintes au pénal ; discriminations de tous ordres ; violences aux biens et personnes ; grèves formelles ou du zèle ; mise en jeu des assurances ; programmes de reconstructions.

7. Un mot sur cet article.

Il ne se veut pas une critique des différentes approches politiques et règlementaires de la protection ainsi que des plans associés; nous avons malheureusement constaté que bons nombres de décideurs ignoraient ce que la conduite d'un exercice associé à un scénario, construit selon les concepts expliqués dans cet article, pouvait leur apporter dans l'évaluation de leurs plans.

Cet article voudrait, aussi, simplement faire évoluer les canevas d'exercices pour y intégrer l'approche « systèmes », l'apport potentiel ou les dangers que représentent les réseaux sociaux formels ou informels, points aujourd'hui très peu évoqués dans les scénarios d'exercice depuis le niveau communal et des entreprises jusqu'à celui de l'Europe.

Nous pensons que tout scénario d'exercice (même au niveau d'un village, d'une petite infrastructure ou d'un système élémentaire) doit intégrer un scénario complet à même d'obliger les cellules de crise à réfléchir, agir et en tirer les leçons comme proposé dans cet article.

Notes de fins

[i] Mr Francis Le Gallou : "Un système est un ensemble, formant une unité cohérente et autonome d'objets réels ou conceptuels (éléments matériels, individus, actions, ...) organisé en fonction d'un but (ou d'un ensemble de buts, objectifs, finalités, projets, ...) au moyen d'un jeu de relations (interactions mutuelles, interactions dynamiques...), le tout immergé dans un environnement."

[ii] Grève des mineurs de charbon au Royaume-Uni 1984-1985 et grève nationale SNCF/RATP de 1995.

[iii] Grève d'enlèvement des ordures à Naples en 2008.

[iv] Tempêtes de décembre 1999 et de janvier 2009 en France ; ouragan KATRINA aux USA..

[v] Défaillance du réseau électrique italien du 28 septembre 2003.

[vi] Attaque réussie par un particulier du réseau de pompage et de distribution d'eau du Queensland (Australie) en 2000.

[vii] Jean Lemoigne / Hervé Zwirn : On appelle systèmes complexes ceux dont les interactions des composants sont non linéaires (les effets ne sont pas proportionnels à la cause). Il est souvent extrêmement difficile, voire impossible, de prédire directement le comportement global ; tous les constituants concourent simultanément à la dynamique d'un comportement devenu holistique : on doit étudier le système comme un tout et non pas comme un ensemble de parties indépendantes.

[viii] Attaque contre l'Estonie en 2007 qui a paralysé en particulier tous les sites gouvernementaux et les échanges bancaires.

[ix] Vol de 94 millions numéros de cartes de crédits et données clients détenus par la société JTX aux USA en 2007

[x] Par exemple, le remodelage des lignes de cars privés pendant les grèves RATP et SNCF et l'évolution des revendications salariales des chauffeurs de poids lourds pendant cette période.

[xi] Dynamique des systèmes complexes - Ecole Centrale de Paris.

[xii] http://www.sciences.ch/htmlfr/mathssociales/mathssdynapop01.php#modeleproiespredateurs

[xiii] http://www.counteract.eu/default.aspx

[xiv] Preparation, Conduct and Evaluation of Exercises to Test Preparedness for a Nuclear or Radiological Emergency - Training Materials Emergency Preparedness and Response 2006

[xv] http://training.fema.gov/emiweb/downloads/IS139ExPlan.doc

[xvi] Guide d'élaboration d'exercices en vue de valider les plans de préparation à une pandémie de grippe, Bureau OMS du Pacifique occidental

[xvii] au sens de la COMMUNICATION DE LA COMMISSION EUROPEENNE sur un programme européen de protection des infrastructures critiques - COM(2006) 786 final

[xviii] Systèmes complexes coopérants (COSY) - Laboratoire de Conception et d'Intégration des Systèmes - Université Pierre Mendes France

[xix] Holisme qui prend en compte la globalité d'une question ; on peut y associer l'approche stochastique qui intègre les incertitudes et les probabilités. Son opposé est l'approche déterministe.

[xx] IN-SPIRE développé par le National Visualization and Analytics Center™ des laboratoires de Pacific Northwest National
i2 Analyst's Notebook (de iBridge)
COPLINK pour l'analyse de réseaux criminels

Références - Bibliographie

[1] Georges-Yves Kervern, Patrick Rubise. *Introduction aux cindyniques.* Economica - 1991
ISBN-13: 978-2717820614
[2] Georges-Yves Kervern. *Eléments fondamentaux des cindyniques.* Economica - 1995
ISBN-13: 978-2717827569
[3] Georges-Yves Kervern, Philippe Boulenger. *Cindyniques - Concepts et mode d'emploi.*Economica - 2007
ISBN-13:978-2717852875
[4] Edgar Morin. *Introduction à la pensée complexe - Précaution, crise, assurance.* Seuil - Nle edition 2005
ISBN-13: 978-2020668378
[5] James Gleick. *La théorie du chaos.* Flammarion - 2008
ISBN-13: 978-2081218048
[6] Chrispohe Letellier. *Le Chaos dans la nature.* Vuibert 2006
ISBN 978-2-7117-9140-8
[7] Michel Bonami, Bernard de Hennin, Jean-Michel Boqué, Jean-Jacques Legrand.
Management des systèmes complexes - *Pensée systémique et intervention dans les organisation*s
De Boeck Université - 1993 ISBN-13: 978-2804117313
[8] Niklas Luhmann. Soziale Systeme: Grundriß einer allgemeinen Theorie. Suhrkamp; Auflage: Neuauflage. (5. August 2008)
ISBN-13: 978-3518282663
[9] Olivier Godard,Claude Henry, Patrick Lagadec, Erwann Michel-Kerjean. *Traité des nouveaux risques - Précaution, crise, assurance*. Gallimard - 2002
ISBN-13: 978-2070421039
[10] David Dufresne. *Maintien de l'ordre: l'Enquête*. Hachette Littérature.2007
[11] NATO. *Joint Analysis Hand Book*. 3rd Version 2007
[12] Le Monde. Scénarios catastrophe pour une grippe fatale 7 mai 2009
[13] Paul K. Davis. *Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis and Transformation*. Rand 2002
[14] Bishop, P. Hines. *The Current State of Scenario Development Foresight Vol 9.* A & Collins, T. (2007)